

CRYPT CLOUD+ :SECURE AND EXPRESSIVE DATA ACCESS CONTROL FOR CLOUD STORAGE

M. Manasa, T. Swaranitha, D. Nikhitha, Mrs. U. Swetha, Assistant Professor
SVS Group Of Institutions, Bheemaram(V), Hanamkonda T.S. India -506015

ABSTRACT

Secure cloud storage, which is an emerging cloud service, is designed to protect the confidentiality of outsourced data but also to provide flexible data access for cloud users whose data is out of physical control. Ciphertext-policy Attribute-Based Encryption (CP-ABE) is regarded as one of the most promising techniques that may be leveraged to secure the guarantee of the service. However, the use of CP-ABE may yield an inevitable security breach which is known as the misuse of access credential (i.e. decryption rights), due to the intrinsic “all-or-nothing” decryption feature of CP-ABE. In this paper, we investigate the two main cases of access credential misuse: one is on the semi – trusted authority side, and the other is on the side of cloud user. To mitigate the misuse, we propose the first accountable authority and revocable CP- ABE based cloud storage system with white-box traceability and auditing, referred to as crypt cloud +. We also present the security analysis and further demonstrate the utility of our system via experiments.

1. INTRODUCTION

The prevalence of cloud computing may indirectly incur vulnerability to the confidentiality of outsourced data and the privacy of cloud users. A particular challenge here is on how to guarantee that only authorized users can gain access to the data, which has been outsourced to cloud, at anywhere and anytime. One naive solution is to employ encryption technique on the data prior to uploading to cloud. However, the solution limits further data sharing and processing. This is so because a data owner needs to download the encrypted data from cloud and further re-encrypt them for sharing (suppose the data owner has no local copies of the data). A fine-grained access control over encrypted data is desirable in the context of cloud computing.

Cipher text-Policy Attribute-Based Encryption (CP-ABE) may be an effective solution to guarantee the confidentiality of data and provide fine-grained access control here. In a CP-ABE based cloud storage system, for example, organizations (e.g., a university such as the University of Texas at San Antonio) and individuals (e.g., students, faculty members and visiting scholars of the university) can first specify access policy over attributes of a potential cloud user. Authorized cloud users then are granted access credentials (i.e., decryption keys) corresponding to their attribute sets (e.g., student

role, faculty member role, or visitor role), which can be used to obtain access to the outsourced data. As a robust one-to-many encryption mechanism, CP-ABE offers a reliable method to protect data stored in cloud, but also enables fine-grained access control over the data. Generally speaking, the existing CP-ABE based cloud storage systems fail to consider the case where access credential is misused. For instance, a university deploys a CPABE based cloud storage system to outsource encrypted student data to cloud under some access policies that are compliant with the relevant data sharing and privacy legislation (e.g., the federal Family Educational Rights and Privacy Act (FERPA) and Health Insurance Portability and Accountability Act of 1992 (HIPAA)).

The official in charge at the organization (e.g. university's security manager) initializes the system parameters and issues access credentials for all users (e.g., students, faculty members, and visiting scholars). Each employee is assigned with several attributes (e.g., "administrator", "senior manager", "financial officer", "tenured faculty", "tenure-track faculty", "non tenure-track faculty", "instructors", "adjunct", "visitor", and/or "students").

Only the employees with attributes satisfying the decryption policy of the outsourced data are able to gain access to the student data stored in cloud (e.g. student admission materials).

As we may have known, the leakage of any sensitive student information stored in cloud could result in a range of consequences for the organization and individuals (e.g., litigation, loss of competitive advantage, and criminal charges).

The CP-ABE may help us prevent security breach from outside attackers. But when an insider of the organization is suspected to commit the "crimes" related to the redistribution of decryption rights and the circulation of student information in plain format for illicit financial list also possible for us to revoke the compromised access privileges? In addition to the above questions, we have one more which is related to key generation authority.

A cloud user's access credential (i.e., decryption key) is usually issued by a semi-trusted authority based on the attributes the user possesses. How could we guarantee that this particular authority will not (re-) distribute the generated access credentials to others? For example, the organization security official leaks a lecturer Alice's key to an outsider Bob (who is not the employee of the university). One potential answer to the question is to employ multiple authorities. Nevertheless, this incurs additional cost in communication and infrastructure deployment and meanwhile, the problem of malicious collusion among authorities remains.

Therefore, we posit that adopting an accountable authority approach to mitigate the access credential

escrow problem is the preferred strategy. Seeking to mitigate access credential misuse, we propose Crypt Cloud +, an accountable authority and revocable CPABE based cloud storage system with white-box traceability and auditing. To the best of our knowledge, this is the first practical solution to secure fine-grained access control over encrypted data in cloud. Specifically, in our work, we first present a CP ABE based cloud storage framework. Using this (generic) framework, we propose two accountable authority and revocable CP-ABE systems (with whitebox traceability and auditing) that are fully secure in the standard model, referred to as ATER-CP-ABE and ATIR-CPABE, respectively. Based on the two systems, we present the construction of CryptCloud+ that provides the following features.

Traceability of malicious cloud users. Users who leak their access credentials can be traced and identified. **Accountable authority.** A semi-trusted authority, who (without proper authorization) generates and further distributes access credentials to unauthorized user(s), can be identified. This allows further actions to be undertaken (e.g. criminal investigation or civil litigation for damages and breach of contract). **Auditing.** An auditor can determine if a (suspected) cloud user is guilty in leaking his/her access credential. “Almost” zero storage requirement for tracing. We use a Paillier-like encryption as an extractable commitment in tracing malicious cloud users and more practically, we do not need to maintain an identity table of users for tracing (unlike the approach used in). **Malicious cloud user’s revocation.** Access credentials for individual traced and further determined to be “compromised” can be revoked. We design two mechanisms to revoke the “traitor(s)” effectively.

The ATER-CP-ABE provides an explicitly revocation mechanism where a revocation list is specified explicitly into the algorithm Encrypt, while the ATIRCP- ABE offers an implicitly revocation where the encryption does not need to know the revocation list but a key update operation is required periodically.

This paper extends our earlier work (a conference version in as follows).

We present a formal framework model of the proposed system, designed for practical cloud storage system deployment. We address a weakness in the auditing procedure of the conference version. Specifically, a malicious user may change tid of his secret key in the conference version, and the auditing procedure will fail in this case. As a mitigation, we revise the key generation algorithm and add an audit list to detect if the tid is changed. We enhance the functionality of the construction (w.r.t. AAT-CP-ABE) proposed in the conference version and further present two enhanced constructions, namely ATER-CP-ABE and ATIR-CP-ABE. These constructions allow us to effectively revoke the malicious users explicitly or implicitly. We also present the new definitions,

technique and related materials of ATER-CP- ABE and ATIR-CP-ABE. Based on the new ATER-CP-ABE and ATIR-CP-ABE, we present Crypt Cloud+ which is an effective and practical solution for secure cloud storage. We provide general extensions (of our system) on the large universe, the multi- use, and the prime-order setting cases, so that the solution introduced in this paper is more scalable in real-world applications. We comprehensively evaluate the efficiency of the proposed ATER-CP-ABE and ATIR-CP-ABE via experiments.

2. LITERATURE SURVEY

L1: Secure and Privacy Preserving Protocol for Cloud-Based Vehicular DTN's Authors: Xiaolei Dong, Xiaolei Dong, Zhenfu Cao, Athanasios Vasilakos **Published year:** 2015.

Description: Cloud-assisted vehicular delay tolerant networks (DTNs) have been utilized in wide-ranging applications where a continuous end-to-end connection is unavailable, the message transmission is fulfilled by the cooperation among vehicular nodes and follows a store-carry-and-forward manner, and the complex computational work can be delegated to the disengaged vehicles in the parking lots which constitute the potential vehicular cloud. Nevertheless, the existing incentive schemes as well as the packet forwarding protocols cannot well model continuous vehicle collaboration, resist vehicle compromise attacks and collusion attacks, leaving the privacy preservation issues untouched. In this paper, a novel threshold credit-based incentive mechanism (TCBI) is proposed based on the modified model of population dynamics to efficiently resist the node compromise attacks, stimulate the cooperation among intermediate nodes, maximize vehicular nodes' interest, and realize the fairness of possessing the same opportunity of transmitting packets for credits. Then, a TCBI- based privacy-preserving packet forwarding protocol is proposed to solve the open problem of resisting layer-adding attack by outsourcing the privacy-preserving aggregated transmission evidence generation for multiple resource-constrained vehicles to the cloud side from performing any one-way trapdoor function only once. The vehicle privacy is well protected from both the cloud and transportation manager. Finally, formal security proof and the extensive simulation show the effectiveness of our proposed TCBI in resisting the sophisticated attacks and the efficiency in terms of high reliability, high delivery ratio, and low average delay in cloud-assisted vehicular DTNs.

L2: Security and Privacy for Cloud-Based IoT: Challenges Authors: Zhenfu Cao, Jun Zhou, Xiaolei Dong, Athanasios v.vasilakos. **Published year:** 2019.

Description: The Internet of Things is increasingly becoming a ubiquitous computing service, requiring huge volumes of data storage and processing. Unfortunately, due to the unique

characteristics of resource constraints, self-organization, and short-range communication in IoT, it always resorts to the cloud for outsourced storage and computation, which has brought about a series of new challenging security and privacy threats. In this article, we introduce the architecture and unique security and privacy requirements for the next generation mobile technologies on cloud-based IoT, identify the inappropriateness of most existing work, and address the challenging issues of secure packet forwarding and efficient privacy preserving authentication by proposing new efficient privacy preserving data aggregation without public key homomorphic encryption. Finally, several interesting open problems are suggested with promising ideas to trigger more research efforts in this emerging area.

L3: Outsourced Attribute-Based Encryption with Keyword Search Function for Cloud Storage

Authors: Jiguo Li , Xiaonan Li , Yichen Zhang, Jinguang Han.

Published year: 2017

Description: Cloud computing becomes increasingly popular for data owners to outsource their data to public cloud servers while allowing intended data users to retrieve these data stored in cloud. This kind of computing model brings challenges to the security and privacy of data stored in cloud. Attribute-based encryption (ABE) technology has been used to design fine-grained access control system, which provides one good method to solve the security issues in cloud setting. However, the computation cost and ciphertext size in most ABE schemes grow with the complexity of the access policy. Outsourced ABE (OABE) with fine-grained access control system can largely reduce the computation cost for users who want to access encrypted data stored in cloud by outsourcing the heavy computation to cloud service provider (CSP). However, as the amount of encrypted files stored in cloud is becoming very huge, which will hinder efficient query processing. To deal with above problem, we present a new cryptographic primitive called attribute-based encryption scheme with outsourcing key-issuing and outsourcing decryption, which can implement keyword search function (KSF-OABE). The proposed KSF-OABE scheme is proved secure against chosen-plaintext attack (CPA). CSP performs partial decryption task delegated by data user without knowing anything about the plaintext. Moreover, the CSP can perform encrypted keyword search without knowing anything about the keywords embedded in trapdoor.

L4: Flexible and Fine-Grained Attribute-Based Data Storage in Cloud Computing

Authors: Jiguo Li, Wei Yao, Yichen Zhang, Huiling Qian, Jinguang Han

Published year: 2017

Description: With the development of cloud computing, outsourcing data to cloud server attracts lots

of attentions. To guarantee the security and achieve flexibly fine-grained file access control, attribute based encryption (ABE) was proposed and used in cloud storage system. However, user revocation is the primary issue in ABE schemes. In this article, we provide a cipher text-policy attribute based encryption (CP-ABE) scheme with efficient user revocation for cloud storage system. The issue of user revocation can be solved efficiently by introducing the concept of user group. When any user leaves, the group manager will update users' private keys except for those who have been revoked. Additionally, CP-ABE scheme has heavy computation cost, as it grows linearly with the complexity for the access structure. To reduce the computation cost, we outsource high computation load to cloud service providers without leaking file content and secret keys. Notably, our scheme can withstand collusion attack performed by revoked users cooperating with existing users. We prove the security of our scheme under the divisible computation Diffie-Hellman assumption. The result of our experiment shows computation cost for local devices is relatively low and can be constant. Our scheme is suitable for resource constrained devices.

L5 : SeDaSC: Secure Data Sharing in Clouds

Authors: Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Athanasios

V. Vasilakos, Keqin Li, Albert Y. Zomaya.

Published year: 2015

Description: Cloud storage is an application of clouds that liberates organizations from establishing in-house data storage systems. However, cloud storage gives rise to security concerns. In case of group-shared data, the data face both cloud-specific and conventional insider threats. Secure data sharing among a group that counters insider threats of legitimate yet malicious users is an important research issue. In this paper, we propose the Secure Data Sharing in Clouds (SeDaSC) methodology that provides: 1) data confidentiality and integrity; 2) access control; 3) data sharing (forwarding) without using compute-intensive reencryption; 4) insider threat security; and 5) forward and backward access control. The SeDaSC methodology encrypts a file with a single encryption key. Two different key shares for each of the users are generated, with the user only getting one share. The possession of a single share of a key allows the SeDaSC methodology to counter the insider threats. The other key share is stored by a trusted third party, which is called the cryptographic server. The SeDaSC methodology is applicable to conventional and mobile cloud computing environments. We implement a working prototype of the SeDaSC methodology and evaluate its performance based on the time consumed during various operations. We formally verify the working of SeDaSC by using high-level Petri nets, the Satisfiability Modulo Theories Library, and a Z3 solver. The results proved to be

encouraging and show that SeDaSC has the potential to be effectively used for secure data sharing in the cloud.

L6:IoT-Based Big Data Storage Systems in Cloud Computing: Perspectives and Challenges

Authors : Hongming Cai, Boyi Xu, Lihong Jiang, and Athanasios V. Vasilakos.

Published year: 2016

Description: Internet of Things (IoT) related applications have emerged as an important field for both engineers and researchers, reflecting the magnitude and impact of data-related problems to be solved in contemporary business organizations especially in cloud computing. This paper first provides a functional framework that identifies the acquisition, management, processing and mining areas of IoT big data, and several associated technical modules are defined and described in terms of their key characteristics and capabilities. Then current research in IoT application is analyzed, moreover, the challenges and opportunities associated with IoT big data research are identified. We also report a study of critical IoT application publications and research topics based on related academic and industry publications. Finally, some open issues and some typical examples are given under the proposed IoT-related research framework.

L7: Enabling Semantic Search Based on Conceptual Graphs over Encrypted Outsourced Data

Authors: Zhangjie Fu, Fengxiao Huang, Xingming Sun, Athanasios Vasilakos, and Ching-Nung Yang

Published year: 2016

Description: Currently, searchable encryption is a hot topic in the field of cloud computing. The existing achievements are mainly focused on keyword-based search schemes, and almost all of them depend on predefined keywords extracted in the phases of index construction and query. However, keyword-based search schemes ignore the semantic representation information of users' retrieval and cannot completely match users' search intention. Therefore, how to design a content-based search scheme and make semantic search more effective and context-aware is a difficult challenge. In this paper, for the first time, we define and solve the problems of semantic search based on conceptual graphs (CGs) over encrypted outsourced data in clouding computing (SSCG). We first employ the efficient measure of “sentence scoring” in text summarization and Tregex to extract the most important and simplified topic sentences from documents. We then convert these simplified sentences into CGs. To perform quantitative calculation of CGs, we design a new method that can map CGs to vectors. Next, we rank the returned results based on “text summarization score”. Furthermore, we propose a basic idea for SSCG and give a significantly improved scheme to satisfy the security

guarantee of searchable symmetric encryption (SSE). Finally, we choose a real-world dataset, i.e., the CNN dataset to test our scheme. The results obtained from the experiment show the effectiveness of our proposed scheme.

L8 : Reducing Trust in the PKG in Identity Based Cryptosystems Authors: Vipul Goyal

Published year: 2007

Description: One day, you suddenly find that a private key corresponding to your Identity is up for sale at e-Bay. Since you do not suspect a key compromise, perhaps it must be the PKG who is acting dishonestly and trying to make money by selling your key. How do you find out for sure and even prove it in a court of law? This paper introduces the concept of Traceable Identity based Encryption which is a new approach to mitigate the (inherent) key escrow problem in identity based encryption schemes. Our main goal is to restrict the ways in which the PKG can misbehave. In our system, if the PKG ever maliciously generates and distributes a decryption key for an Identity, it runs the risk of being caught and prosecuted. In contrast to other mitigation approaches, our approach does not require multiple key generation authorities.

L9 : Traceable CP-ABE with Short Cipher texts: How to Catch People Selling Decryption Devices on eBay Efficiently

Authors: Jianting Ning, Zhenfu Cao, Xiaolei Dong, Junqing Gong Jie Chen

Published year: 2016

Description: Cipher text-policy attribute-based encryption (CP-ABE) is a highly promising solution for cloud computing, which has been widely applied to provide fine-grained access control in cloud storage services recently. However, for CP-ABE based cloud storage systems, if a decryption device appears on eBay described and advertised to be able to decrypt any cipher texts with policies satisfied by an attribute set or even with a specific access policy only, no one can trace the malicious user(s) who built such a decryption device using their private key(s). This has been known as a major obstacle to deploying CP-ABE systems in real-world commercial applications. Due to the one-to-many encryption mechanism of CP-ABE, the same decryption privilege is shared by multiple users who have the same attributes. It is difficult to identify the malicious user(s) who built such a decryption device. To track people selling decryption devices on eBay efficiently, in this paper, we develop a new methodology for constructing traitor tracing functionality, and present the first black-box traceable CP-ABE (BT-CP-ABE) with short cipher texts which are independent of the number of users \mathcal{N} . The black-box traceability is public, fully collusion-resistant, and adaptively traceable against both key-like decryption black-box and policy-specific decryption black-box.

3. PROBLEM STATEMENT

The current landscape of cloud storage solutions predominantly revolves around centralized platforms offered by major service providers such as Google Drive, Dropbox and Amazon S3. These platforms offer users the convenience of storing and accessing data remotely over the internet, facilitating seamless collaboration and data sharing. However, the existing systems often employ conventional access control mechanisms such as role-based access control (RBAC) or access control lists (ACLs), which may not provide the necessary granularity for nuanced data access control. Furthermore, while encryption is commonly used to protect data during transit and storage, it may not be fully utilized to its potential to ensure end-to-end security. Additionally, the centralized nature of these systems raises concerns about data privacy and security, as users relinquish control of their data to third-party providers. As a result, there is a growing demand for more secure and expressive data access control mechanisms that empower users to retain control over their data while leveraging the benefits of cloud storage.

4. PROPOSED SYSTEM:

The proposed system aims to address the limitations of existing cloud storage solutions by introducing a Crypt Cloud Secure and Expressive Data Access Control framework. This framework integrates advanced cryptographic techniques with fine-grained access control mechanisms to enhance the security and flexibility of cloud storage systems. By leveraging cryptographic protocols such as homomorphic encryption and attribute-based encryption, sensitive data can be encrypted and processed securely while preserving confidentiality and integrity. Additionally, the system will implement expressive data access control policies, allowing users to define intricate access rules based on various attributes such as user roles, data classifications, and temporal constraints. Through the combination of cryptographic security measures and expressive access controls, the proposed system aims to provide a robust and customizable solution for securing data in the cloud. Furthermore, by decentralizing access control and encryption processes, the system mitigates the risks associated with centralized storage platforms, empowering users to maintain sovereignty over their data. Overall, the proposed system represents a significant advancement in cloud storage security, offering organizations and individuals greater control and confidence in their data management practices.

5. FUTURE SYSTEM

In envisioning the future of cloud storage systems, there is a notable trajectory towards the integration of emerging technologies and paradigms aimed at further enhancing security, scalability, and efficiency. The future system foresees the incorporation of cutting-edge advancements such as

quantum-resistant cryptography, decentralized storage architectures, and artificial intelligence-driven security mechanisms. Quantum-resistant cryptography will play a pivotal role in fortifying data encryption against the potential threat posed by quantum computing, ensuring long-term resilience against cryptographic attacks. Decentralized storage architectures, facilitated by blockchain technology or similar distributed ledger technologies, will democratize data storage by enabling peer-to-peer sharing and eliminating single points of failure inherent in centralized cloud platforms. Moreover, artificial intelligence and machine learning algorithms will be leveraged to bolster security measures through proactive threat detection, anomaly detection, and automated incident response. These intelligent systems will continuously adapt and evolve to counter emerging cyber threats, ensuring robust defense mechanisms for safeguarding sensitive data in the cloud. Additionally, the future system will prioritize interoperability and standardization, fostering seamless integration between disparate cloud environments and facilitating data portability and mobility. By embracing these advancements, the future cloud storage system will redefine the boundaries of security, accessibility, and innovation, ushering in a new era of trust and reliability in cloud computing infrastructures.

5.1 ADVANTAGES

Robust Data Security:

Advanced cryptographic techniques ensure encryption of sensitive data, both in transit and at rest. Protection against unauthorized access and data breaches.

Fine-Grained Access Control

Granular control over data access permissions based on user roles, data attributes, and temporal constraints. Precise definition of access policies enhances data privacy and facilitates compliance with regulatory requirements.

Decentralization:

Reduced reliance on centralized authorities reduces the risks associated with single points of failure. Enhances resilience against attacks and ensures continuity of service.

User Empowerment:

Users retain sovereignty over their data, reducing dependence on third-party service providers. Fosters trust and accountability in cloud storage environments.

Compliance Readiness:

Facilitates compliance with data protection regulations such as GDPR and HIPAA through customizable access controls. Enables organizations to adhere to regulatory requirements with ease.

6. Architecture Diagram

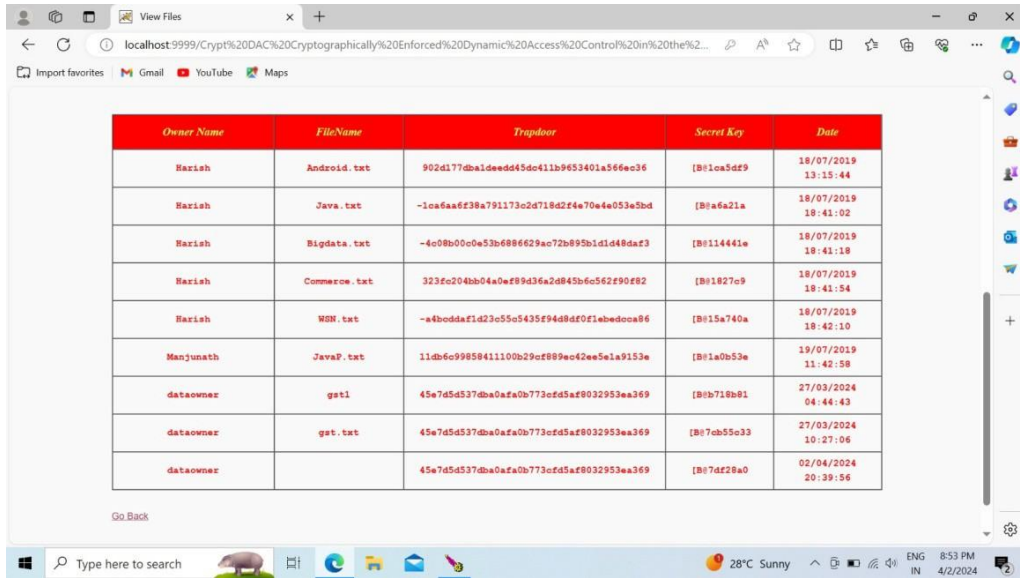


Architecture Diagram

7. OUTCOMES RESULTS

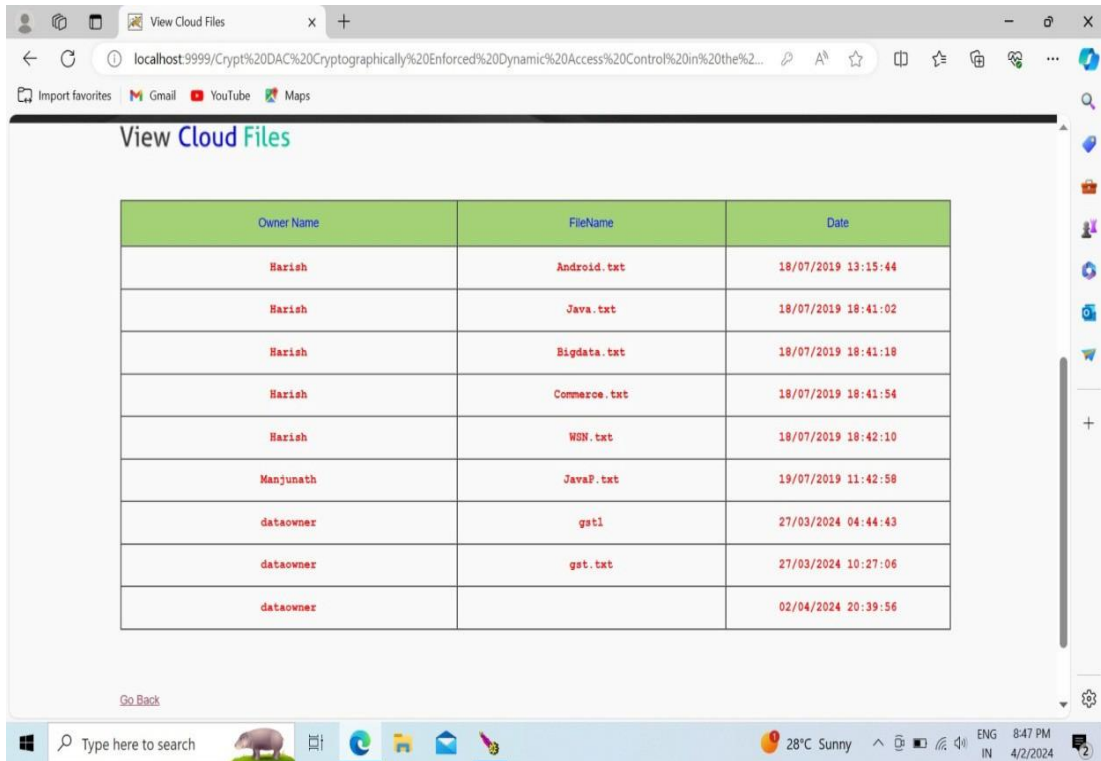


End user screen shot



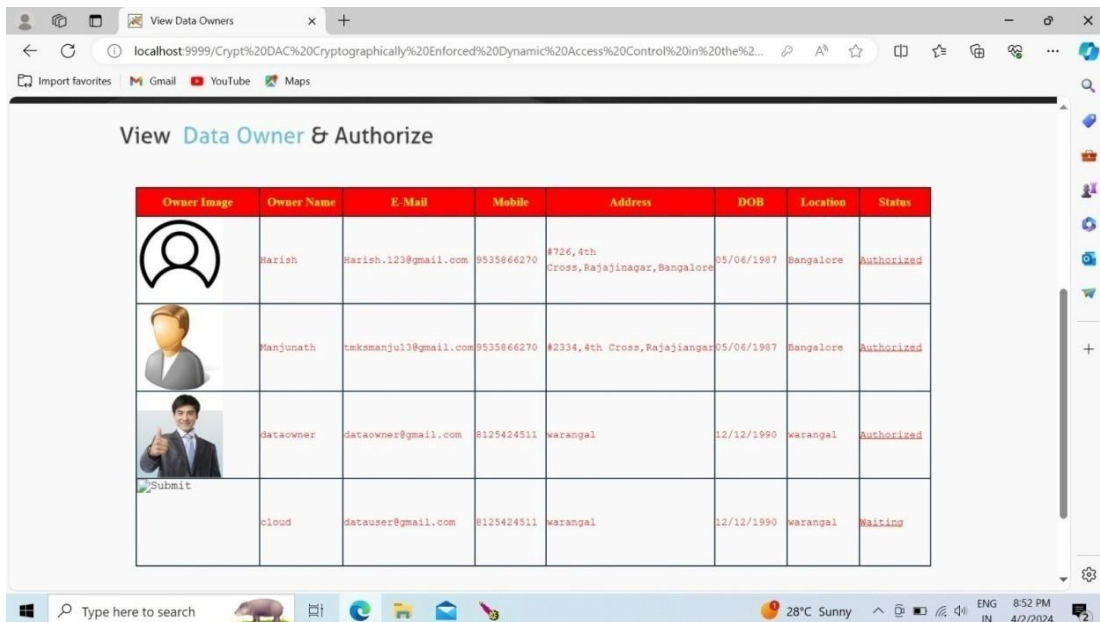
Owner Name	FileName	Trapdoor	Secret Key	Date
Haxiah	Android.txt	902d177dba1deed45dc411b9653401a566ec36	[B@1ca5df9	18/07/2019 13:15:44
Haxiah	Java.txt	-1ca6aa6f38a791173c2d718d2f4e70e4e053e5bd	[B@a6a21a	18/07/2019 18:41:02
Haxiah	Bigdata.txt	-4c08b00c0e53b6886629ac72b895b1d1d48daf3	[B@114441e	18/07/2019 18:41:18
Haxiah	Commerce.txt	323fc204bb04a0ef99d36a2d845b6c56290f82	[B@1827e9	18/07/2019 18:41:54
Haxiah	WSN.txt	-a4b0daf1d23c55c5435f94d8df0f1ebdcca86	[B@15a740a	18/07/2019 18:42:10
Manjunath	JavaP.txt	11db6c99859411100b29cf899ec42ee5e1a9153e	[B@1a0b53e	19/07/2019 11:42:58
dataowner	get1	45e7d5d537dba0afa0b773cfd5af8032953ea369	[B@b718b81	27/03/2024 04:44:43
dataowner	get.txt	45e7d5d537dba0afa0b773cfd5af8032953ea369	[B@7cb55c33	27/03/2024 10:27:06
dataowner		45e7d5d537dba0afa0b773cfd5af8032953ea369	[B@7df28a0	02/04/2024 20:39:56





Data Owner Screen Shot



Owner Name	FileName	Date
Harish	Android.txt	18/07/2019 13:15:44
Harish	Java.txt	18/07/2019 18:41:02
Harish	Bigdata.txt	18/07/2019 18:41:18
Harish	Commerce.txt	18/07/2019 18:41:54
Harish	WSN.txt	18/07/2019 18:42:10
Manjunath	JavaP.txt	19/07/2019 11:42:58
dataowner	gst1	27/03/2024 04:44:43
dataowner	gst.txt	27/03/2024 10:27:06
dataowner		02/04/2024 20:39:56

Cloud Files



Owner Image	Owner Name	E-Mail	Mobile	Address	DOB	Location	Status
	Harish	Harish.123@gmail.com	9535866270	#726,4th Cross,Rajajinagar,Bangalore	05/06/1987	Bangalore	Authorized
	Manjunath	makmanjul3@gmail.com	9535866270	#2334,4th Cross,Rajajinagar	05/06/1987	Bangalore	Authorized
	dataowner	dataowner@gmail.com	8125424511	warangal	12/12/1990	warangal	Authorized
	cloud	datauser@gmail.com	8125424511	warangal	12/12/1990	warangal	Waiting

Data Owner & authorized Screen shot

View FR

localhost:9999/Crypt%20DAC%20Cryptographically%20Enforced%20Dynamic%20Access%20Control%20in%20the%2...

View Access Control for File Secret Key

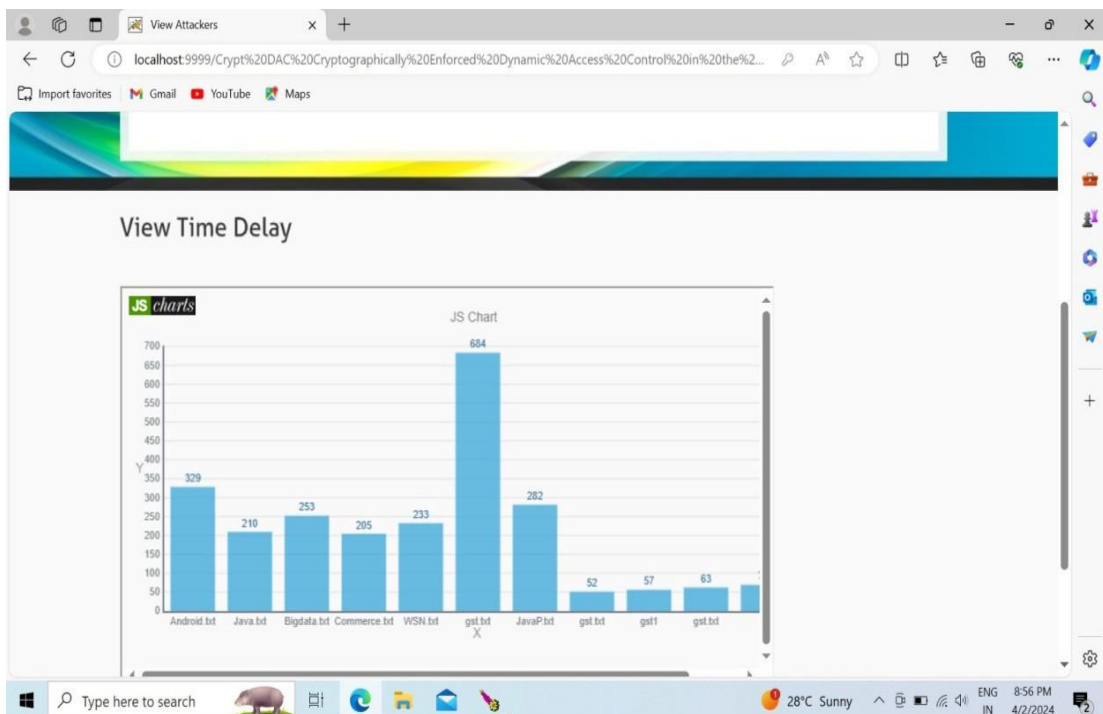
User Name	File Name	Owner Name	Req Date	Res Date	Permitted Trapdoor	Sk	Status
datauser	gst.txt	owner	27/03/2024 04:35:24	27/03/2024 04:35:49	45e7d5d537dba0afa0b773ofdf5af8032953ea369	[B@211fcab2	Yes
datauser	gst.txt	owner	27/03/2024 04:36:17	Waiting for Response	req	req	No
datauser	gst.txt	owner	27/03/2024 11:00:04	Waiting for Response	req	req	No
datauser	gst.txt	owner	27/03/2024 11:01:09	Waiting for Response	req	req	No
datauser	gst.txt	owner	27/03/2024 11:12:32	Waiting for Response	req	req	No
datauser	gst.txt	owner	28/03/2024	Waiting for	req	req	No

Type here to search

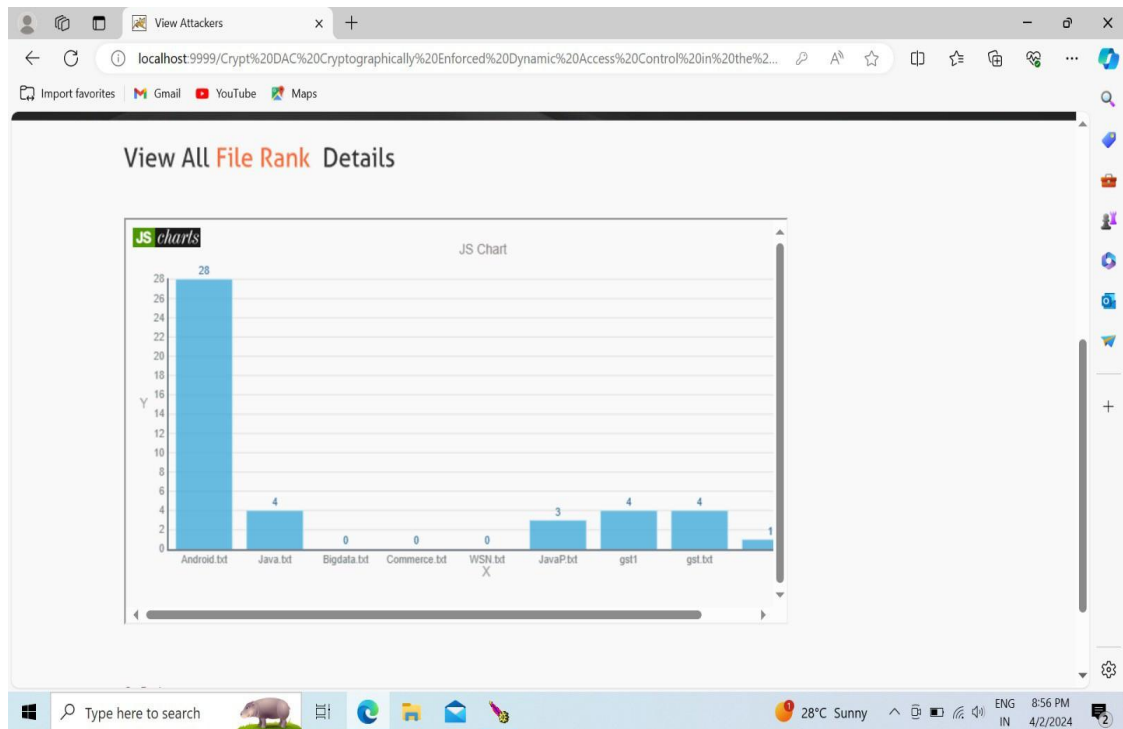
28°C Sunny

ENG IN 8:50 PM 4/2/2024

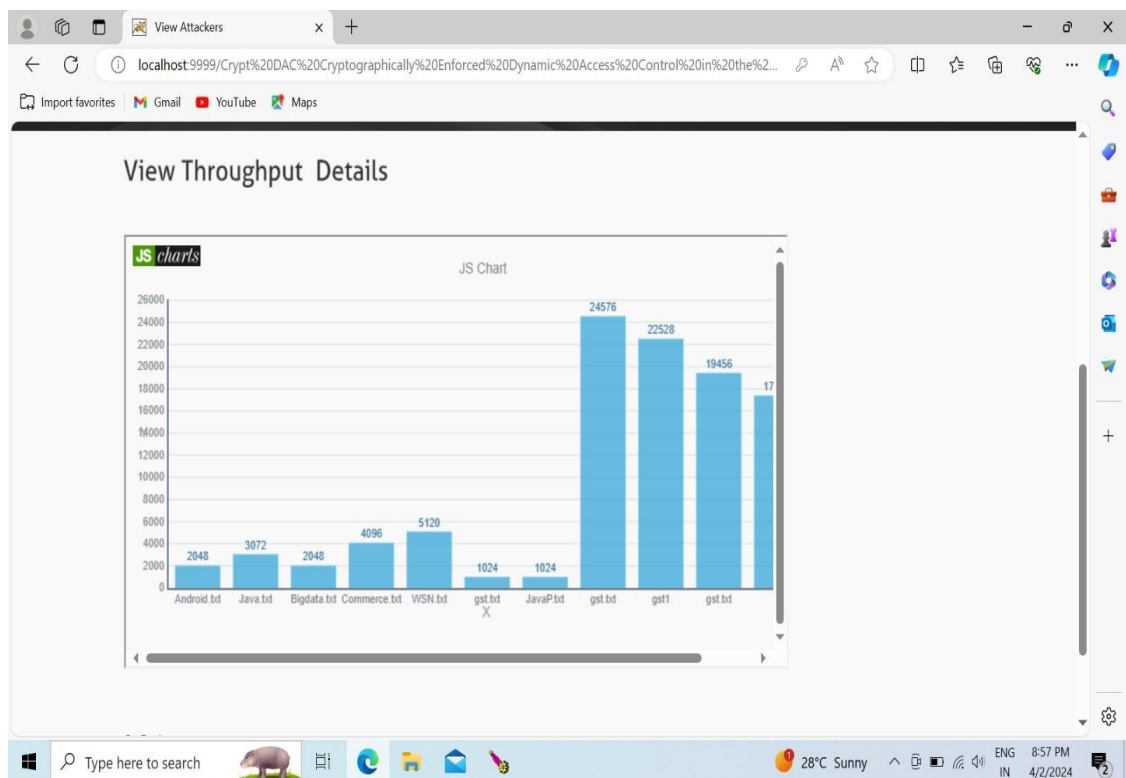
Access control for file secret key



Bar Graph of JS



Bar Graph of Throughput details



File rank details

8. CONCLUSION

In this work, we have addressed the challenge of credential leakage in CP-ABE based cloud storage system by designing an accountable authority and revocable Crypt Cloud which supports white-box traceability and auditing (referred to as Crypt Cloud+). This is the first CP-ABE based cloud storage system that simultaneously supports white-box traceability, accountable authority, auditing and effective revocation. Specifically, CryptCloud+ allows us to trace and revoke malicious cloud users (leaking credentials). Our approach can be also used in the case where the users' credentials are redistributed by the semi-trusted authority. We note that we may need black-box traceability, which is a stronger notion (compared to white-box traceability), in Crypt Cloud. One of our future works is to consider the black-box traceability and auditing. Furthermore, AU is assumed to be fully trusted in CryptCloud+. However, in practice, it may not be the case. Is there any way to reduce trust from AU? Intuitively, one method is to employ multiple AUs. This is similar to the technique used in threshold schemes. But it will require additional communication and deployment cost. Meanwhile, the problem of collusion among AUs remains. Another potential approach is to employ secure multi-party computation in the presence of malicious adversaries. However, the efficiency is also a bottleneck. Designing efficient multi-party computation and decentralizing trust among AUs (while maintaining the same level of security and efficiency) is also a part of our future work. We use Paillier-like encryption to serve as an extractable commitment to achieve white-box traceability. From an abstract view point, any extractable commitment may be employed to achieve white-box traceability in theory. To improve the efficiency of tracing, we may make use of a more light-weight (pairing-suitable) extractable commitment. Also, the trace algorithm in CryptCloud+ needs to take the master secret key as input to achieve white-box traceability of malicious cloud users. Intuitively, the proposed CryptCloud+ is private traceable. Private traceability only allows the tracing algorithm to be run by the system administrator itself, while partial/full public traceability enables the administrator, authorized users and even anyone without the secret information of the system to fulfill the trace. Our future work will include extending CryptCloud+ to provide "partial" and fully public traceability without compromising on performance.

9. FUTURE ENHANCEMENT

Looking towards future enhancements, several avenues present themselves for further advancing the capabilities and effectiveness of the Crypt Cloud Secure and Expressive Data Access Control system. One potential area of improvement involves the integration of machine learning and artificial intelligence algorithms to enhance threat detection and anomaly detection capabilities. By leveraging

AI-driven analytics, the system can proactively identify and mitigate potential security threats, thereby bolstering its overall resilience against cyber attacks. Additionally, the system could benefit from the incorporation of block chain technology to further decentralize data storage and access control processes. By leveraging blockchain's immutable and distributed ledger capabilities, the system can provide an even higher level of data integrity and transparency, reducing the risk of data manipulation or unauthorized access. Furthermore, future enhancements could focus on expanding the system's interoperability and compatibility with emerging technologies and cloud platforms, enabling seamless integration with a broader ecosystem of applications and services. Moreover, ongoing research and development efforts can explore advancements in cryptographic protocols and techniques to further strengthen data security and privacy protections. Overall, these future enhancements hold the potential to propel the Crypt Cloud Secure and Expressive Data Access Control system to new heights of security, scalability, and innovation, ensuring its continued relevance and effectiveness in meeting the evolving needs of users and organizations in the digital age.

10. REFERENCES

- [1] Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li, and Albert Y. Zomaya. Sedasc: Secure data sharing in clouds. *IEEE Systems Journal*, 11(2):395–404, 2017.
- [2] MazharAli, Samee U. Khan and Athanasios V. Vasilakos. Security in cloud computing: Opportunities and challenges. *Inf. Sci.*, 305:357–383, 2015.
- [3] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, et al. A view of cloud computing. *Communications of the ACM*, 53(4):50–58, 2010.
- [4] Nuttapong Attrapadung and Hideki Imai. Attribute-based encryption supporting direct/indirect revocation modes. In *Cryptography and Coding*, pages 278–300. Springer, 2009.
- [5] Amos Beimel. Secure schemes for secret sharing and key distribution. PhD thesis, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.
- [6] Mihir Bellare and Oded Goldreich. On defining proofs of knowledge. In *Advances in Cryptology-CRYPTO'92*, pages 390–420. Springer, 1993.

- [7] Dan Boneh and Xavier Boyen. Short signatures without random oracles. In EUROCRYPT - 2004, pages 56–73, 2004.
- [8] Hongming Cai, Boyi Xu, Lihong Jiang, and Athanasios V. Vasilakos. Iot-based big data storage systems in cloud computing: Perspectives and challenges. IEEE Internet of Things Journal, 4(1):75–87, 2017.
- [9] Jie Chen, Romain Gay, and Hoeteck Wee. Improved dual system ABE in prime-order groups via predicate encodings. In Advances in Cryptology - EUROCRYPT 2015, pages 595–624, 2015.
- [10] Angelo De Caro and Vincenzo Iovino. jpbcc: Java pairing based cryptography. In ISCC 2011, pages 850–855. IEEE, 2011.
- [11] Hua Deng, Qianhong Wu, Bo Qin, Jian Mao, Xiao Liu, Lei Zhang, and Wenchang Shi. Who is touching my cloud. In Computer Security-ESORICS 2014, pages 362–379. Springer, 2014.
- [12] Zhangjie Fu, Fengxiao Huang, Xingming Sun, Athanasios Vasilakos, and Ching-Nung Yang. Enabling semantic search based on conceptual graphs over encrypted outsourced data. IEEE Transactions on Services Computing, 2016.
- [13] Vipul Goyal. Reducing trust in the PKG in identity based cryptosystems. In Advances in Cryptology-CRYPTO2007, pages 430–447. Springer, 2007.
- [14] Vipul Goyal, Steve Lu, Amit Sahai, and Brent Waters. Black-box accountable authority identity-based encryption. In Proceedings of the 15th ACM conference on Computer and communications security, pages 427–436. ACM, 2008.
- [15] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM conference on Computer and communications security, pages 89–98. ACM, 2006.
- [16] Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu, and Dechao Qiu. Security of the internet of things: perspectives and challenges. Wireless Networks, 20(8):2481–2501, 2014.
- [17] Allison Lewko. Tools for simulating features of composite order bilinear groups in the prime order setting. In Advances in Cryptology–EUROCRYPT 2012, pages 318–335. Springer, 2012.
- [18] Allison Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product

encryption. In *Advances in Cryptology– EUROCRYPT 2010*, pages 62–91. Springer, 2010.

[19] Allison Lewko and Brent Waters. New proof methods for attribute-based encryption: Achieving full security through selective techniques. In *Advances in Cryptology–CRYPTO 2012*, pages 180–198. Springer, 2012. [20] Jiguo Li, Xiaonan Lin, Yichen Zhang, and Jinguang Han. KSFOABE: outsourced attribute-based encryption with keyword search function for cloud storage. *IEEE Trans. Services Computing*, 10(5):715–725, 2017.

[21] JiguoLi,WeiYao,YichenZhang,HuilingQian,andJinguangHan. Flexible and fine-grained attribute-based data storage in cloud computing. *IEEE Trans. Services Computing*, 10(5):785–796, 2017.

[22] Jin Li, Qiong Huang, Xiaofeng Chen, Sherman SM Chow, Duncan S Wong, and Dongqing Xie. Multi-authority ciphertext-policy attribute-based encryption with accountability. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ASIACCS 2011*, pages 386–390. ACM, 2011.

[23] Jin Li, Kui Ren, and Kwangjo Kim. A2be: Accountable attribute based encryption for abuse free access control. *IACR Cryptology ePrint Archive*, 2009:118, 2009.

[24] Jiaqiang Liu, Yong Li, Huandong Wang, Depeng Jin, Li Su, Lieguang Zeng, and Thanos Vasilakos. Leveraging software defined networking for security policy enforcement. *Inf. Sci.*, 327:288–299, 2016.

[25] QiangLiu,HaoZhang,JiafuWan,andXinChen. An access control model for resource sharing based on the role-based access control intended for multi-domain manufacturing internet of things. *IEEE Access*, 5:7001–7011, 2017.

[26] Zhen Liu, Zhenfu Cao, and Duncan S Wong. Blackbox traceable cp-abe: how to catch people leaking their keys by selling decryption devices on ebay. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 475–486. ACM, 2013.